

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-152194

(43)Date of publication of application : 24.05.2002

(51)Int.Cl.

H04L 9/32  
H04H 1/00  
H04H 1/02  
H04L 9/08  
H04N 7/167

(21)Application number : 2000-344384

(71)Applicant : TOSHIBA CORP  
MATSUSHITA ELECTRIC IND CO  
LTD

(22)Date of filing : 10.11.2000

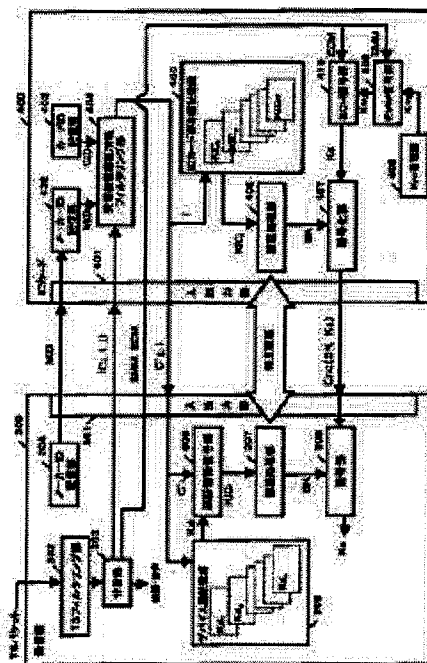
(72)Inventor : OI SHINICHI  
KUROIWA WATARU  
KUMAZAKI HIROJI  
SAIJO TAKESHI  
INOUE TETSUYA  
MATSUO TAKASHI  
MURAKAMI HIRONORI  
FUDA YUICHI  
OMORI MOTOJI

(54) LIMITED RECEPTION DEVICE, LIMITED RECEPTION DEVICE AUTHENTICATING METHOD, AND CIPHER COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a limited reception device which actualizes mutual authentication of high reliability even if a reception device main body and a security module do not hold a common global secret.

SOLUTION: The reception device main body is equipped with a storage means which stores an ID for identifying a maker, a storage means which stores one or more pieces of information unique to the reception device main body, a deciphering means which decipheres information ciphered by using as a key the reception device main body unique information, and an authentication processing means which performs authentication processing with the security module by inputting the information outputted by the deciphering means. The security module is equipped with a storage means which stores a card ID for uniquely identifying the limited reception device, a means which filters reception device authentication information by referring to the maker ID and card ID, a storage means which stores one or more pieces of unique to the security module, and an authentication processing means which performs authentication processing with the reception device main body by inputting the security module unique information.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-152194  
(P2002-152194A)

(43)公開日 平成14年5月24日(2002.5.24)

(51)Int.Cl. <sup>7</sup>	識別記号	F.I	キーワード*(参考)
H 0 4 L 9/32		H 0 4 H 1/00	F 5 C 0 6 4
H 0 4 H 1/00		1/02	E 5 J 1 0 4
1/02		H 0 4 L 9/00	6 7 5 A
H 0 4 L 9/08			6 0 1 C
H 0 4 N 7/167		H 0 4 N 7/167	Z
審査請求 未請求 請求項の数27 OL (全 22 頁)			

(21)出願番号 特願2000-344384(P2000-344384)

(22)出願日 平成12年11月10日(2000.11.10)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 大井 伸一

神奈川県横浜市磯子区新杉田町8番地

株式会社東芝横浜事業所内

(74)代理人 100090446

弁理士 中島 司朗 (外1名)

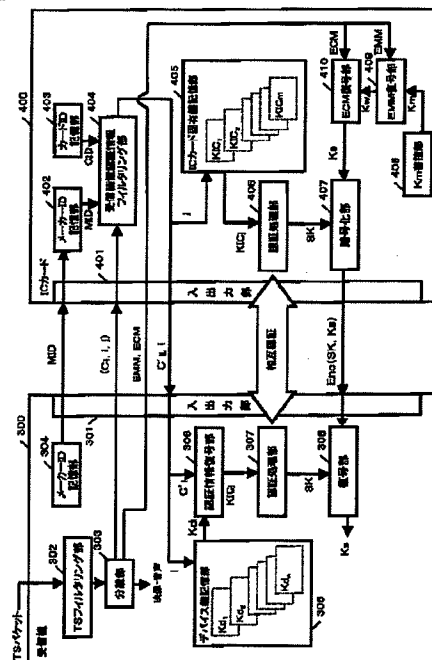
最終頁に続く

(54)【発明の名称】 限定受信装置、限定受信装置認証方法及び暗号通信方法

(57)【要約】

【課題】 受信装置本体とセキュリティモジュールとが共通のグローバルシークレットを保持せずとも、信頼性が高い相互の認証を実現する限定受信装置を提供する。

【解決手段】 受信装置本体は、メーカーを識別するIDを記憶する記憶手段と、1つ以上の受信装置本体固有情報を記憶する記憶手段と、受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールは、限定受信装置を一意に識別するカードIDを記憶する記憶手段と、メーカーIDとカードIDとを参照して受信装置認証情報をフィルタリングする手段と、1つ以上のセキュリティモジュール固有情報を記憶する記憶手段と、セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行う認証処理手段を備える。



## 【特許請求の範囲】

【請求項1】 放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置の受信装置本体であって、セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、

1つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備することを特徴とする受信装置本体。

【請求項2】 前記メーカーIDを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段を具備することを特徴とする請求項1に記載の受信装置本体。

【請求項3】 放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置のセキュリティモジュールであって、

受信装置本体とのデータ入出力を行う入出力手段と、限定受信装置を一意に識別するカードIDを記憶するカードID記憶手段と、

前記カードIDを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とするセキュリティモジュール。

【請求項4】 受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段をさらに具備し、前記フィルタリング手段は、メーカーIDとカードIDとを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングすることを特徴とする請求項3に記載のセキュリティモジュール。

【請求項5】 前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項3及び請求項4の

いずれか一項に記載のセキュリティモジュール。

【請求項6】 放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、

受信装置本体は、セキュリティモジュールとのデータ入出力を行う入出力手段と、

10 受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、

1つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、セキュリティモジュールは、

20 受信装置本体とのデータ入出力を行う入出力手段と、限定受信装置を一意に識別するカードIDを記憶するカードID記憶手段と、

受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、

前記メーカーIDと前記カードIDとを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

30 1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とする限定受信装置。

【請求項7】 前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項6に記載の限定受信装置。

【請求項8】 放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、

受信装置本体は、セキュリティモジュールとのデータ入出力を行う入出力手段と、

受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、

50 前記メーカーIDを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリン

グ手段と、

1つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、

前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、

セキュリティモジュールは、

受信装置本体とのデータ入出力を行う入出力手段と、

限定受信装置を一意に識別するカードIDを記憶するカードID記憶手段と、

前記カードIDを参照して、受信装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段とを具備することを特徴とする限定受信装置。

【請求項9】 前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項8に記載の限定受信装置。

【請求項10】 受信装置本体にセキュリティモジュールが装着されている限定受信装置の認証方法であって、限定受信装置が、受信した放送波に含まれる受信装置認証情報を分離するステップと、

自受信装置宛の受信装置認証情報だけを取り出すフィルタリング処理ステップと、

受信装置本体が、前記受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成するステップと、受信装置本体とセキュリティモジュールが、受信装置本体とセキュリティモジュールとが共有した前記セキュリティモジュール固有情報を用いて認証処理を行うステップを有することを特徴とする受信装置認証方法。

【請求項11】 前記受信装置認証情報は、受信装置本体が1つ以上保持する受信装置本体固有情報のいずれか1つを鍵として、セキュリティモジュールが1つ以上保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報のいずれか1つを暗号化することにより生成される情報と、

受信装置本体のメーカーを識別するメーカーIDと、

受信装置を識別するカードIDとを含み、

受信装置認証情報の生成に用いた受信装置本体固有情報及びセキュリティモジュール固有情報を特定するためのインデックス情報に組み合わせて、放送局設備から放送波を用いて送出されることを特徴とする、請求項10に

記載の受信装置認証方法。

【請求項12】 前記フィルタリング処理は、前記メーカーIDとセキュリティモジュールが記憶しているカードIDとが一致する受信装置認証情報を自受信装置宛の受信装置認証情報として選択することを特徴とする請求項10及び請求項11のいずれか一項に記載の受信装置認証方法。

【請求項13】 受信装置本体で生成される前記共有情報は、前記受信装置本体固有情報を鍵として、前記受信装置認証情報に含まれる情報を復号することにより復元されることを特徴とする、請求項10から請求項12のいずれか一項に記載の受信装置認証方法。

【請求項14】 前記フィルタリング処理は、受信装置本体において、受信装置本体が記憶しているメーカーIDと一致する受信装置認証情報を選択し、セキュリティモジュールにおいて、セキュリティモジュールが記憶しているカードIDと一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項10から請求項13のいずれか一項に記載の受信装置認証方法。

【請求項15】 セキュリティモジュールは、セキュリティモジュールが受信装置本体に装着された後に受信装置本体から入力されるメーカーIDを記憶するステップを有することを特徴とする、請求項10から請求項13のいずれか一項に記載の受信装置認証方法。

【請求項16】 前記フィルタリング処理は、セキュリティモジュールにおいて、前記記憶されたメーカーIDとセキュリティモジュールが記憶しているカードIDとが一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項15に記載の受信装置認証方法。

【請求項17】 セキュリティモジュールは、フィルタリング処理により抽出した受信装置認証情報を記憶するステップを有し、セキュリティモジュールが受信装置本体に装着された後に受信装置本体から入力されるメーカーIDが前記記憶している受信装置認証情報に含まれるメーカーIDと等しい場合は、前記記憶している受信装置認証情報を受信装置本体に出力し、受信装置本体は、セキュリティモジュールから渡された前記受信装置認証情報を基に前記共有情報を生成することを特徴とする、請求項14から請求項16のいずれか一項に記載の受信装置認証方法。

【請求項18】 認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と、乱数を出力する乱数生成手段と、

前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いてセキュリティモジュールから入力される情報を復号する復号手段とをさらに具備することを特徴とする、請求項1及び請求項2のいずれか一項に記

載の受信装置本体。

【請求項19】 前記暗号鍵を用いてセキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備することを特徴とする、請求項18に記載の受信装置本体。

【請求項20】 認証処理手段が出力した受信装置本体との共有値を記憶する記憶手段と、  
前記記憶している共有値と受信装置本体から入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、  
前記暗号鍵を用いて受信装置本体へ出力する情報を暗号化する暗号化手段とをさらに具備することを特徴とする、請求項3から請求項5のいずれか一項に記載のセキュリティモジュール。

【請求項21】 前記暗号鍵を用いて受信装置本体から入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項20に記載のセキュリティモジュール。

【請求項22】 放送されてきた信号を受信してセキュリティモジュールに出力する受信装置本体と、受信装置本体から入力されたデータを処理して受信装置本体に処理データを出力するセキュリティモジュールとを構成要素に含む限定受信装置であって、  
受信装置本体は、  
セキュリティモジュールとのデータ入出力を行う入出力手段と、  
受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、  
1つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、  
前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、  
前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行い、セキュリティモジュールとの共有値を出力する認証処理手段と、  
前記認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と、  
乱数を出力する乱数生成手段と、  
前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、  
前記暗号鍵を用いてセキュリティモジュールから入力される情報を復号する復号手段とを具備し、  
セキュリティモジュールは、  
受信装置本体とのデータ入出力を行う入出力手段と、  
限定受信装置を一意に識別するカードIDを記憶するカードID記憶手段と、  
受信装置本体から入力される、受信装置本体のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、  
前記メーカーIDと前記カードIDとを参照して、受信

装置本体から入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、  
前記セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行って受信装置本体との共有値を出力する認証処理手段と、  
前記認証処理手段が出力した受信装置本体との共有値を記憶する記憶手段と、

10 前記記憶している共有値と受信装置本体から入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、  
前記暗号鍵を用いて受信装置本体へ出力する情報を暗号化する暗号化手段とを具備することを特徴とする限定受信装置。

【請求項23】 前記受信装置本体は、  
前記暗号鍵を用いてセキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備し、  
前記セキュリティモジュールは、  
20 前記暗号鍵を用いて受信装置本体から入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項22に記載の限定受信装置。

【請求項24】 受信装置本体にセキュリティモジュールが装着されている限定受信装置の受信装置本体とセキュリティモジュール間の暗号通信方法であって、  
受信装置本体は、セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップを有し、  
セキュリティモジュールは、受信装置本体との認証処理によって生成した共有値を記憶するステップを有し、  
30 受信装置本体及びセキュリティモジュールは、それぞれが記憶した共有値を鍵として用いて暗号通信を行うことを特徴とする、暗号通信方法。

【請求項25】 受信装置本体にセキュリティモジュールが装着されている限定受信装置の受信装置本体とセキュリティモジュール間の暗号通信方法であって、  
受信装置本体は、  
セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップと、  
乱数を生成するステップと、  
40 前記乱数をセキュリティモジュールに出力するステップと、  
前記記憶したセキュリティモジュールとの共有値と前記乱数とを用いて暗号鍵を生成するステップとを有し、  
セキュリティモジュールは、  
受信装置本体との認証処理によって生成した共有値を記憶するステップと、  
前記記憶した受信装置本体との共有値と受信装置本体から入力された乱数とを用いて暗号鍵を生成するステップと、  
50 前記暗号鍵を受信装置本体との共有値として記憶するス

トップとを有し、  
受信装置本体及びセキュリティモジュールは、それぞれ  
が生成した暗号鍵を用いて暗号通信を行うことを特徴と  
する、暗号通信方法。

【請求項26】 受信装置本体は、前記生成した暗号鍵  
をセキュリティモジュールとの新しい共有値として記憶  
するステップをさらに有し、

セキュリティモジュールは、前記生成した暗号鍵を受信  
装置本体との新しい共有値として記憶するステップをさ  
らに有することを特徴とする、請求項25に記載の暗号  
通信方法。

【請求項27】 受信装置本体からセキュリティモジュ  
ールへのコマンド送信をトリガーとして、受信装置本体  
が前記乱数を生成することを特徴とする、請求項25及  
び請求項26のいずれか一項に記載の暗号通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、視聴契約を必要と  
する放送システム（限定受信システム）の限定受信装置  
に関し、特に、受信装置本体にセキュリティモジュール  
が装着される限定受信装置、限定受信装置の認証方法、  
及び暗号通信方法に関する。

【0002】

【従来の技術】従来の標準的な限定受信方法であるMP  
EG2 SYSTEMS（ISO/IEC13818-  
1）では、送出側は、映像や音声等のコンテンツをスク  
ランブル鍵Ksでスクランブルして送信し、また、この  
スクランブル鍵KsをECM（Entitlement Control Me  
ssages：番組情報）に格納した後、このECMをワーク  
鍵Kwで暗号化して送信する。また、ワーク鍵Kwは、  
事前にEMM（Entitlement Management Messages：個  
別情報）に格納され、個別鍵Kmで暗号化されて送信さ  
れる。

【0003】図1は、この送出側の構成を示している。  
映像や音声等のコンテンツを生成するコンテンツ生成部  
100と、Ksを生成するKs生成部101と、コンテ  
ンツをKsでスクランブルするスクランブラ106と、  
Ksを格納したECMを生成するECM生成部102  
と、Kwを生成するKw生成部103と、Kwを用いて  
ECMを暗号化するECM暗号化部107と、Kwを格  
納したEMMを生成するEMM生成部104と、Kmを  
生成するKm生成部105と、Kmを用いてEMMを暗  
号化するEMM暗号化部108と、スクランブルされた  
コンテンツや暗号化されたECM及びEMMを多重化す  
る多重化部109とを備えている。

【0004】ECMには、Ksの他に、番組識別情報で  
ある番組ティア情報や現在時刻が格納され、これらがK  
wで暗号化される。また、ECMには、非暗号のモジュ  
ール識別フラグが付される。また、EMMには、Kwの  
他に、該当する受信装置の視聴権を識別するための個別

ティア情報や視聴契約の情報が格納され、これらがKm  
で暗号化される。また、EMMには、非暗号のモジュ  
ール識別フラグ及び該当する受信装置のIDが付される。

【0005】多重化部で多重化された信号はTSパケッ  
ト（Transport Stream Packet）に変換されて送出され  
る。一方、番組を視聴する受信側の構成は、図2に示す  
ように、受信装置本体（受信機）110と、受信機に装  
着されるICカード等のセキュリティモジュール120  
とを備えており、受信機は選局されたTSパケットだけ  
を取り込むTSフィルタリング部111と、多重されて  
いる信号を分離する分離部112と、スクランブルされ  
たコンテンツを復号化するデスクランブラ113とを具  
備し、また、セキュリティモジュールは、Kmを保持す  
るKm蓄積部121と、Kmを用いてEMMを復号する  
EMM復号部122と、Kwを用いてECMを復号する  
ECM復号部123とを具備している。

【0006】受信機は、自己宛のEMMが送られてくる  
とこれを受信する。EMMは、視聴契約の更新等に伴っ  
て送られて来る。このEMMは、分離部112で分離さ  
れてEMM復号部122に出力され、EMM復号部は、  
Km蓄積部121に蓄積されているKmを用いてこれを  
復号し、EMMに含まれるKw、個別ティア情報及び契  
約情報などをECM復号部123に出力する。ECM復  
号部は、これらの情報を保持する。

【0007】受信機が、スクランブルされたコンテンツ  
と、そのスクランブル鍵Ksを含むECMとを受信する  
と、スクランブルされたコンテンツは、分離部112で  
分離されてデスクランブラ113に送られ、また、分離  
されたECMはECM復号部123に送られる。ECM  
復号部は、このECMを、前記保持したKwで復号化  
し、そこに含まれた現在時刻を視聴契約の有効期間と比  
較し、また、番組ティア情報を個別ティア情報と比較し  
て、チャンネル視聴権の有無を識別する。そして、チャ  
ンネル視聴権が認められる場合にだけ、復号したKsを  
受信機のデスクランブラ113に出力する。受信機のデ  
スクランブラは、セキュリティモジュールから送られて  
くるKsを順次取得し、コンテンツのスクランブルを解  
く。こうしてスクランブルされた番組の視聴が可能にな  
る。

【0008】しかし、この場合、セキュリティモジュ  
ールから受信機に非暗号の状態のKsが渡されるため、そ  
の通信路上でKsが不正に取得され、視聴契約をしてい  
ない者がコンテンツのデスクランブルにKsを不正利用  
する恐れがある。特開平09-46672号公報には、  
こうした点を改善するため、セキュリティモジュールと  
受信機とが共通鍵を保持し、セキュリティモジュールは  
Ksを共通鍵で暗号化して受信機に送り、受信機はこれ  
を共通鍵で復号してKsを取り出す方式が記載されてい  
る。この場合、共通鍵がセキュリティモジュールから受  
信機へ渡される際に不正に取得される恐れがあり、この

共通鍵が不正に取得されると、結局、Ksが不正に取得されてしまう。

【0009】特開平02-195376号公報には、ICカード間での安全な鍵共有方法が記載されている。それによると、第2のICカードが乱数を生成し、その乱数をマスタ鍵で暗号化して第1のICカードに渡し、第1のICカードは前記の暗号化された乱数をマスタ鍵で復号して乱数を復元し、第1のICカードと第2のICカードは共有した前記乱数をセッション鍵として暗号通信を行う。この場合、第1のICカードと第2のICカードは予めグローバルシークレットであるマスタ鍵を共有しているので、乱数を安全に共有することが可能である。

【0010】

【発明が解決しようとする課題】これまでの説明から明らかなように、受信装置本体とセキュリティモジュールとの間で安全な暗号通信を行うためには、受信装置本体とセキュリティモジュールとが、共有情報を安全に共有することが重要である。予め共有情報をグローバルシークレットとして受信装置本体とセキュリティモジュールとに格納した場合、セッション毎に相互認証を行うことにより、セッション毎に異なる安全なセッション鍵を共有することが可能である。しかし、この場合、悪意を持つ者が受信装置とセキュリティモジュールとの間で通信される相互認証用データ（チャレンジ・レスポンス等）を不正取得して暗号解読を試み、万が一、共有情報の割り出しに成功すると、セッション鍵の割り出しが可能となり、その結果、スクランブル鍵Ksや、視聴契約情報、課金情報といった受信装置本体とセキュリティモジュールとの間で通信されるデータが不正に取得されてしまう。また、割り出された共有情報は、全ての受信装置において共通であるため、限定受信システム運用に与えるダメージは非常に重大である。システム運用を回復するための対処として、新しい共有情報を暗号化して格納した記憶メディアを全視聴者に配布して受信機及びセキュリティモジュールの共有情報を更新する方法が考えられるが、これは膨大なコストの発生を伴うと予想され、非現実的である。

【0011】また、受信装置本体とICカード等のセキュリティモジュールの製造は、それぞれ複数の異なるメーカーが担当するのが一般的である。予め共有情報を受信装置本体及びセキュリティモジュールに格納しておく場合、全てのメーカー製の受信装置本体と、全てのメーカー製のセキュリティモジュールとの組み合わせにおいて相互認証を正しく行うためには、メーカーを問わず、全ての受信機及びセキュリティモジュールで等しい共有情報を共有する必要がある。この場合、ある1つのメーカーにおける機密情報管理レベルが低く、メーカー内部から共有情報の漏洩が発生してしまうと、他のメーカー製の受信装置本体及びセキュリティモジュールにもその影響が波及し、限定受信システムの運用に致命的なダメージ

を及ぼすことになる。

【0012】本発明は、こうした問題点を解決するものであり、受信装置本体とセキュリティモジュールとで予め共通の共有情報を持たずとも、セッション鍵生成等で用いる共有情報を安全に共有することができる限定受信装置の認証方法、及び、限定受信装置を提供することを目的とする。

【0013】

【課題を解決するための手段】この課題を解決するために本発明は、受信装置本体にセキュリティモジュールが装着される構成を取る限定受信装置において、受信装置本体は受信装置本体を製造するメーカーを識別するIDを記憶するメーカーID記憶手段と、1つ以上の受信装置本体固有情報を記憶する受信装置本体固有情報記憶手段と、前記受信装置本体固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールは限定受信装置を一意に識別するカードIDを記憶するカードID記憶手段と、メーカーIDとカードIDとを参照して受信装置認証情報をフィルタリングするフィルタリング手段と、1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、セキュリティモジュール固有情報を入力として受信装置本体との認証処理を行う認証処理手段を備えることを特徴とする。

【0014】また、放送局設備において受信装置認証情報を生成し、受信装置認証情報を放送局から放送波を用いて送出し、限定受信装置は受信した受信装置認証情報からメーカーIDとカードIDを検索キーとして自受信装置宛の受信装置認証情報だけをフィルタリングし、受信装置本体はフィルタリングした受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成して、受信装置本体とセキュリティモジュールは前記共有情報を用いて認証処理を行う。

【0015】また、受信装置認証情報は、受信装置本体が保持する受信装置本体固有情報を鍵としてセキュリティモジュールが保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報を暗号化することにより生成される情報と、受信装置本体のメーカーを識別するメーカーIDと、受信装置を識別するカードIDとから構成する。

【0016】以上により、受信装置本体とセキュリティモジュールとでセキュリティモジュール固有情報を共有し、その共有情報を基に、受信装置本体とセキュリティモジュールとの間の暗号通信に用いるセッション鍵を生成する。また、受信装置本体は乱数生成手段と、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備え、セキュリティモジュールは、セッショ

ン鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備える。

【0017】また、受信装置本体は乱数を生成してセキュリティモジュールに出力すると共に、セッション鍵記憶手段から読み出したセッション鍵と前記乱数とから暗号鍵を生成する。さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。セキュリティモジュールは、受信装置本体から入力した乱数と、セッション鍵記憶手段から読み出したセッション鍵とから暗号鍵を生成する、さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。

【0018】以上により、受信装置本体とセキュリティモジュールとで共通の暗号鍵を共有し、暗号通信を行う。

【0019】

【発明の実施の形態】本発明の実施の形態について、図を用いて説明する。なお、以降では、受信装置本体を受信機、セキュリティモジュールをICカード、受信装置本体固有情報をデバイス鍵、セキュリティモジュール固有情報をICカード固有鍵と記述して説明する。

【0020】図3は、放送局で管理するデバイス鍵及びICカード固有鍵をそれぞれ受信機及びICカードに格納する手順の一例を示す図である。放送局200の一設備である鍵管理センタ201は、受信機メーカー毎に固有の $n$ 個のデバイス鍵 $Kd_i$  ( $1 \leq i \leq n$ ) を生成する。ここで、 $i$  はデバイス鍵のインデックス番号である。 $n$  の値については後述する。

【0021】デバイス鍵の値は受信機メーカー毎に異なる。同一のメーカーが製造する全ての受信機には同じ値のデバイス鍵 $Kd_1 \sim Kd_n$  が格納される。デバイス鍵生成部202で生成された各デバイス鍵は、鍵管理センタ内のデバイス鍵DB203に受信機メーカーを識別するメーカーIDと共に登録され、安全に管理される。例えば、第3者の立ち入りが制限された機密情報管理室にて管理される。

【0022】受信機メーカー206は、放送局から安全な手段により配送される自メーカー用のデバイス鍵を受け取り、デバイス鍵を受信機207の製造時に受信機内部のデバイス鍵記憶部に格納する。放送局から受信機メーカーへのデバイス鍵配送は、例えば、CD-ROMのような記録メディアに暗号化したデバイス鍵を記録し、オフライン配送する。

【0023】1つの受信機には $n$ 個のデバイス鍵が格納される。なお、受信機内部のデバイス鍵記憶部をデータの取り出しが困難なLSI内部等に具備することにより、悪意ある受信機ユーザによるデバイス鍵暴露の可能性を低くすることができる。また一方、鍵管理センタは、ICカード毎に固有の $m$ 個のICカード固有鍵 $KI_Cj$  ( $1 \leq j \leq m$ ) を生成する。ここで、 $j$  はICカー

ド固有鍵のインデックス番号である。 $n$  及び $m$  の値は、セキュリティ的観点や受信機及びICカードの記憶容量等から限定受信システム仕様として規定される。 $n$  及び $m$  の値が大きいほどセキュリティ度は高まるが、受信機及びICカードの記憶容量が多く必要となるため、コスト的に不利となる。

【0024】ICカード固有鍵の値は、ICカードメーカーの区別なく、製造発行される全てのICカード毎に異なる。ICカード固有鍵生成部204で生成された各ICカード固有鍵は、鍵管理センタ内のICカード固有鍵DB205にICカードを識別するカードIDと共に登録され、デバイス鍵と同様に安全に管理される。なお、ICカード固有鍵の値は、製造ロット単位で異なるとしても構わない。

【0025】ICカードメーカー208は、放送局から安全な手段により配送されるICカード固有鍵を受け取り、ICカード固有鍵をICカード製造時にICカード内部のICカード固有鍵記憶部に格納する。一般にICカードは耐タンパ性を有しており、ICカード内のICカード固有鍵記憶部への外部からのアクセスは困難であり、ICカードからICカード固有鍵が暴露される可能性は低い。

【0026】なお、図3ではデバイス鍵を放送局側にて生成して、受信機メーカーに配布する形態となっているが、各受信機メーカーが自メーカーのデバイス鍵を生成し、放送局の鍵管理センタに登録する形態としても構わない。また、図3では鍵管理センタが放送局内の一設備とする構成になっているが、放送局とは独立した構成となってもよい。

【0027】図4は、受信装置認証情報を生成する方法を示す図である。鍵管理センタ201の受信装置認証情報生成部210には、デバイス鍵DB203からデバイス鍵及びメーカーID、ICカード固有鍵DB205からICカード固有鍵及びカードIDが入力される。暗号化部211は、ICカード固有鍵 $KI_Cj$  に対しデバイス鍵 $Kd_i$  を鍵として共通鍵暗号で暗号化した $Enc(Kd_i, KI_Cj)$  を生成して出力する。ここで、 $Enc(X, Y)$  は、データ $Y$  を鍵 $X$  で暗号化した暗号化データを表わす。さらに、暗号化部が出力した前記暗号化データにメーカーIDとICカードIDを付加することにより、受信装置認証情報 $C_{ij} = Enc(Kd_i, KI_Cj) | MID | CID$  となる。ここで $X | Y$  は、データ $X$  とデータ $Y$  を結合したデータを表わす。ある一つの受信機メーカーが製造する受信機と、一つのICカードとの組み合わせに対する受信装置認証情報は、 $C_{11}, C_{12}, \dots, C_{1n}, C_{21}, C_{22}, \dots, C_{mn}$  の合計 $n \times m$  個が生成される。

【0028】図5は、放送波を用いて受信装置認証情報を受信装置側へ送出する、送信側のブロック図である。 $(C_{ij}, i, j)$  生成部130では受信装置確認情報 $C$



$i_j$  とそのインデックス情報  $i$  及び  $j$  とを組み合わせとしたデータ  $(C_{ij}, i, j)$  を生成する。そして、スクランブル鍵  $K_s$  でスクランブルされたコンテンツに個別鍵  $K_m$  で暗号化した EMM とワーク鍵  $K_w$  で暗号化した ECM を多重化すると同様に、多重化部 131 において  $(C_{ij}, i, j)$  をコンテンツ等と多重化し、その信号を TS パケットに変換し放送波として送出する。なお、 $(C_{ij}, i, j)$  を ECM や EMM に格納して放送波として送出する形態であっても構わない。

【0029】図6は、受信した受信装置認証情報を用いて受信装置と IC カードとの間で IC カード固有鍵を共有し、共有した IC カード固有鍵を用いて相互認証を実行してセッション鍵を共有してスクランブル鍵  $K_s$  を暗号通信する方法を説明するブロック図である。まず、IC カード 400 は、受信機 300 に接続された際の初期処理において、受信機がメーカー ID 記憶部 304 に記憶している受信機のメーカー ID (MID) を受け取り、メーカー ID 記憶部 402 に MID を記憶する。受信機が受信した放送波 (TS パケット) は、分離部 303 において、映像・音声信号、EMM、ECM、 $(C_{ij}, i, j)$  に分離される。受信機は、放送波に含まれる全ての  $(C_{ij}, i, j)$  を入出力部 301 から IC カードに送信し、IC カードでは、入出力部 401 において受信した  $(C_{ij}, i, j)$  を受信装置認証情報フィルタリング部 404 に入力する。受信装置認証情報フィルタリング部では、メーカー ID 記憶部 402 に記憶された MID とカード ID 記憶部 403 に記憶されている CID とを参照して、全ての  $(C_{ij}, i, j)$  のうちから MID と CID の両方が一致する  $C_{ij}$  ( $= \text{Enc}(K_{di}, K_{IC_j}) \mid \text{MID} \mid \text{CID}$ )、 $i$  及び  $j$  の組み合わせを抽出する。MID または CID が一致しない  $(C_{ij}, i, j)$  は破棄する。IC カードは、抽出した  $C_{ij}$  から MID と CID とを取り除いた  $C'_{ij}$  ( $= \text{Enc}(K_{di}, K_{IC_j})$ ) と  $i$  とを入出力部 401 から受信機に送信する。また、 $j$  の値に対応する IC カード固有鍵  $K_{IC_j}$  を IC カード固有鍵記憶部 405 から読み出す。

【0030】受信機は IC カードから  $C'_{ij}$  及び  $i$  を受信すると、まず  $i$  の値に対応するデバイス鍵  $K_{di}$  をデバイス鍵記憶部 305 から読み出す。次に、認証情報復号部 306 において、 $K_{di}$  を鍵として  $C'_{ij}$  を復号し、IC カード固有鍵  $K_{IC_j}$  を得る。ここで、受信機の認証情報復号部で用いられる暗号アルゴリズムは、放送局の鍵管理センタで受信装置認証情報を生成した際に用いた共通鍵暗号アルゴリズムに等しい。なお、前記暗号アルゴリズムは、公開鍵暗号アルゴリズムであってもよい。

【0031】このように、受信機と IC カードにおいて、予め共有した情報を持たない状態から IC カード固有鍵  $K_{IC_j}$  を安全に共有することが可能である。さら

に、受信機の認証処理部 307 と IC カードの認証処理部 406 は、前記共有した IC カード固有鍵  $K_{IC_j}$  を用いた相互認証を実行し、セッション鍵  $S_K$  を生成して共有する。IC カードは、受信機から EMM を受け取ると EMM 復号部 409 で  $K_m$  蓄積部 408 に記憶している個別鍵  $K_m$  で EMM を復号して得たワーク鍵  $K_w$  を ECM 復号部に出力し、また、受信機から ECM を受け取ると ECM 復号部 410 で前記  $K_w$  を用いて ECM を復号してスクランブル鍵  $K_s$  を得る。IC カードの暗号化部 407 は前記  $S_K$  を暗号化鍵として  $K_s$  を暗号化した  $\text{Enc}(S_K, K_s)$  を受信機に出力する。受信機の復号部 308 は前記  $S_K$  を復号鍵として、IC カードから受信した前記  $\text{Enc}(S_K, K_s)$  を復号し、スクランブル鍵  $K_s$  を出力する。

【0032】このように、認証処理の度に更新されるセッション鍵  $S_K$  を用いた暗号通信が可能のため、スクランブル鍵  $K_s$  を IC カードから受信機へ高いセキュリティを維持して送信することができる。図7は、受信機と IC カードとのチャレンジ・レスポンスによる相互認証フローの一例を示す図である。以下の説明において、受信機側処理は受信機 300 の相互認証部 310 で、IC カード側の処理は IC カード 400 の相互認証部 413 で行われる。受信機は乱数  $R_1$  を生成して IC カードに送信する。また、受信機は  $K_{IC_j}$  を鍵として  $R_1$  を暗号化し、 $\text{Enc}(K_{IC_j}, R_1)$  を生成する。IC カードは  $R_1$  を受信すると、 $K_{IC_j}$  を鍵として  $R_1$  を暗号化し、 $\text{Enc}(K_{IC_j}, R_1)$  を生成する。さらに乱数  $R_2$  を生成して、 $\text{Enc}(K_{IC_j}, R_1)$  及び  $R_2$  を受信機に送信する。また、IC カードは  $K_{IC_j}$  を鍵として  $R_2$  を暗号化し、 $\text{Enc}(K_{IC_j}, R_2)$  を生成する。受信機は、IC カードから  $\text{Enc}(K_{IC_j}, R_1)$  及び  $R_2$  を受信すると、既に受信機にて作成済みの  $\text{Enc}(K_{IC_j}, R_1)$  と IC カードから受信した  $\text{Enc}(K_{IC_j}, R_1)$  を比較して、値が一致することを確認する。前記  $\text{Enc}(K_{IC_j}, R_1)$  の値が一致した場合、 $K_{IC_j}$  を鍵として IC カードから受信した  $R_2$  を暗号化して  $\text{Enc}(K_{IC_j}, R_2)$  を生成し、IC カードへ送信する。IC カードは、受信機から  $\text{Enc}(K_{IC_j}, R_2)$  を受信すると、既に IC カードにて作成済みの  $\text{Enc}(K_{IC_j}, R_2)$  と IC カードから受信した  $\text{Enc}(K_{IC_j}, R_2)$  を比較して、値が一致することを確認する。そして、受信機と IC カードはそれぞれ、 $R_1$  と  $R_2$  を合成した  $R_1 \cdot R_2$  に対し、 $K_{IC_j}$  を鍵として暗号化することにより、セッション鍵  $S_K$  を得る。ここで、受信機と IC カードそれぞれの相互認証部が備える暗号アルゴリズムは等しい。

【0033】なお、上記チャレンジ・レスポンスによる相互認証フローは一例に過ぎず、 $K_{IC_j}$  を共有秘密情報として用い、その他の相互認証方式を適用してセッ

ョン鍵SKを共有してもよい。また、受信機またはICカードの片方向認証であってもよい。また、セッション鍵SKは、受信機の電源投入時、受信機へのICカード挿入時などのタイミングで、相互認証し共有するものであるが、相互認証において、受信機およびICカードが個々に生成している乱数が相互認証を行う都度異なることがセキュリティ上重要である。すなわち、受信機がICカードを認証する場合を考えると、上記タイミングで生成する乱数R1が、その都度異なる乱数であれば、以前の相互認証に使用したものと同一KICjをもし使用する場合であっても、Enc(KICj, R1)は異なるデータとなり、不正なICカードが、正規ICカードが相互認証に使用した過去のデータを流用してなりすまそうとしても不可能であり、なりすましの不正を防止することが可能となる。同様にICカードが受信機を認証する場合にも、乱数R2が、その都度異なる乱数であれば、以前の相互認証に使用したものと同一KICjを使用する場合であっても、Enc(KICj, R2)は異なるデータとなり、不正な受信機が、正規受信機が相互認証に使用した過去のデータを流用して、なりすまそうとしても不可能であり、なりすましの不正を防止することが可能となる。

【0034】以上説明した、相互認証の際に同じ乱数が生成されないようにするための方法として、不揮発メモリ回路の利用がある。すなわち、乱数生成器が、生成した状態を不揮発メモリに記憶しておき、次回生成する乱数はその状態から継続生成することで同じ乱数の生成を防ぐものである。あるいは、乱数生成器が、初期化データを与え、乱数を得る構成とし、今回生成した乱数を記憶しておき、次回の初期化データとすることにより同じ乱数の生成を防ぐものである。

【0035】図8は、図6で説明した構成において、ICカード400に受信装置認証情報記憶部411を備えた場合を示す図である。ICカードの受信装置認証情報フィルタリング部404では、メーカーID記憶部402に記憶されているMIDとカードID記憶部403に記憶されているCIDとを参照して、全ての(Cij, i, j)のうちからMIDとCIDが一致するCij, i及びjの組み合わせを抽出する。MIDまたはCIDが一致しない(Cij, i, j)は破棄する。そして、抽出したCijからMIDとCIDとを取り除いたC'ij及びiを受信機に送信すると共に、送信したC'ijとi、j、及び前記抽出したCijに含まれていたMIDを受信装置認証情報記憶部411に記憶する。

【0036】図9は、ICカードが受信機に装着された後に認証処理に至るまでの処理フローを示す図である。ICカードの処理フローにおいて、受信装置認証情報記憶部を備えていない場合のフローを実線矢印で、受信装置認証情報記憶部を備えている場合のフローを破線矢印で記述している。受信機においては、ICカードに受信

装置認証情報記憶部を備えている場合と、備えていない場合とで処理フローに違いはない。受信機は、ICカードが装着されると、MIDをICカードに送信する(ステップS100)。そして、放送波に含まれる(Cij, i, j)を検出すると、ICカードに送信する(ステップS101)。その後、ICカードからC'ij, iが入力されると、デバイス鍵記憶部からデバイス鍵Kdiを読み出し、Kdiを鍵としてC'ijを復号してKICjを得て(ステップS103)、そのKICjを用いてICカードとの認証処理を実行する(ステップS104)。

【0037】一方、ICカードにおいては、受信装置認証情報記憶部を備えている場合と、備えていない場合とで処理フローが異なる。まず、ICカードに受信装置認証情報記憶部を備えていない場合のフローを説明する。ICカードは、受信機からMIDを受け取り、メーカーID記憶部に記憶する(ステップS110)。そして、受信機から(Cij, i, j)が入力されるのを待つ(ステップS111)。(Cij, i, j)が入力されると、MIDとCIDの一致するCijを抽出してC'ijを作成し(ステップS112)、C'ijとiを受信機に出力する(ステップS113)。さらに、ICカード固有鍵記憶部から前記jに対応するKICjを読み出し(ステップS114)、そのKICjを用いて受信機との認証処理を実行する(ステップS115)。

【0038】次に、ICカードに受信装置認証情報記憶部を備えている場合のフローを説明する。ICカードは、受信機からMIDを受け取ると、メーカーID記憶部にMIDを記憶する(ステップS110)。そして、受信装置認証情報記憶部からC'ij, i, j、及びMIDの読み出しを試みる(ステップS120)。受信装置認証情報記憶部にC'ij, i, j、及びMIDが記憶されていて、読み出しに成功した場合は、受信機から受け取った前記MIDと比較する(ステップS121)。MIDが等しい場合、受信装置認証情報記憶部から読み出したC'ijとiを受信機に出力する(ステップS113)。ステップS120において受信装置認証情報記憶部にC'ij, i, j、及びMIDが記憶されていない場合、または、ステップS121において前記MIDの比較結果が等しくない場合は、受信機から(Cij, i, j)が入力されるのを待って(ステップS111)、フィルタリング処理によりC'ijを作成する(ステップS112)。そして、C'ij, i, j、及びMIDを受信装置認証情報記憶部に記憶した後(ステップS122)、C'ijとiを受信機に出力する(ステップS113)。その後は、受信装置認証情報記憶部を備えている場合と同様である。

【0039】このように、ICカードに受信装置認証情報記憶部を備えて、受信機に送信したC'ij, i, j、及び受信機のMIDを記憶しておく、次回以降にICカードを装着した際に受信機のメーカーが前回と同じ場

合、受信機からの受信装置認証情報受信を待つことなく、すみやかに受信機との相互認証を開始することができる。

【0040】図10は、図6で説明した構成において、受信機300にも受信装置認証情報フィルタリング部309を備えた場合を示す図である。受信機の受信装置認証情報フィルタリング部309は、分離部303によって分離された $(C_{ij}, i, j)$ のうちから、MIDが一致しない $C_{ij}$ を破棄し、メーカーIDが一致した $C_{ij}$ と $i$ 及び $j$ の組み合わせだけをICカードに送信する。ICカードの受信装置認証情報フィルタリング部412は、受信した $(C_{ij}, i, j)$ のうちからCIDが一致する $C_{ij}$ と $i$ 及び $j$ の組み合わせだけを抽出し、CIDが一致しない $C_{ij}$ は破棄する。

【0041】このように、受信機にも受信装置認証情報フィルタリング部を備えた場合、ICカードに送信する $(C_{ij}, i, j)$ の数を削減することができ、ICカードの受信装置認証情報フィルタリング部での処理量を削減することができるため、ICカードの処理負荷を低減することが可能である。一般に、ICカードと比較して受信機は処理能力が高いので、受信装置認証情報フィルタリング部を備えても大きな負荷増とはならない。また、ICカードにメーカーID記憶部が不必要となる利点がある。

【0042】図11は、受信機とICカードが暗号通信する方法を説明するブロック図である。まず、受信機がICカードに対してコマンドを送信し、そのレスポンスとしてICカードからの暗号化された通信データを受信機が受信する処理について説明する。たとえば、受信機がECMを受信した場合、受信機はECM受信コマンドをICカードにECMと共に送信し、そのレスポンスとして暗号化されたスクランブル鍵 $K_s$ を受信する。

【0043】受信機及びICカードは、ICカード固有鍵 $K_{IC}$ を基に相互認証処理を行って、それぞれセッション鍵 $SK$ を保持する。受信機は $SK$ 記憶部320に、ICカードは $SK$ 記憶部420に $SK$ を記憶する。受信機の乱数生成部321は、乱数 $R$ を生成する。コマンド生成部322は、ユーザによる操作や、放送波受信をトリガーとしてICカードへのコマンドを生成する。その際、前記乱数 $R$ をコマンドデータの一部として構成し、コマンド $COM(R)$ をICカードに送信する。ここで $COM(X)$ は、データ $X$ を含んだコマンドデータを示す。また、受信機の暗号鍵生成部323は、 $SK$ 記憶部に記憶されているセッション鍵 $SK$ と前記乱数 $R$ を入力として暗号鍵 $SK'$ を生成し、復号部308に出力する。さらに、暗号鍵生成部323は前記生成した $SK'$ を $SK$ 記憶部320に出力し、 $SK$ を更新する。復号部308は、ICカードからコマンドに対するレスポンスを受信するまで暗号鍵 $SK'$ を保持する。一方、ICカードのコマンド解析部421は、受信機から受信し

た前記コマンド $COM(R)$ の内容を解析し、乱数 $R$ を取り出して暗号鍵生成部422に出力する。暗号鍵生成部は $SK$ 記憶部422に記憶されているセッション鍵 $SK$ とコマンド解析部から入力された乱数 $R$ から暗号鍵 $SK'$ を生成して暗号化部407に出力する。さらに、暗号鍵生成部422は、前記生成した $SK'$ を $SK$ 記憶部420に出力し、 $SK$ を更新する。ここで、受信機の暗号鍵生成部323と、ICカードの暗号鍵生成部422との暗号鍵生成アルゴリズムは等しい。暗号化部407は、受信機から入力された前記コマンドに対するレスポンスデータ $RES$ を $SK'$ を鍵として暗号化した $Enc(SK', RES)$ を出力し、入出力部401から受信機へ送信する。受信機は、入出力部301がコマンドに対するレスポンスとしてICカードから $Enc(SK', RES)$ を受信すると、復号部308は前記保持していた $SK'$ を鍵として復号し、レスポンスデータ $RES$ を出力する。

【0044】次に、受信機がICカードに対してコマンドを送信し、続けて、暗号化した通信データをICカードへ送受信する処理について説明する。たとえば、番組視聴の課金に関する情報や著作権に関する情報等、不正に取得されると悪用される恐れのある情報をICカード内に蓄えたい場合、受信機はその旨を通知するコマンドをICカードに送信し、さらにそれらの情報を暗号化して送信する。

【0045】受信機の暗号鍵生成部323、及びICカードの暗号鍵生成部422が $SK'$ を生成し、それぞれ $SK$ 記憶部320及び420に $SK'$ を記憶して $SK$ を更新するところまでは、前述のICカードからの通信データを受信機が受信する処理についての説明と同様である。しかし、受信機の暗号鍵生成部323は $SK'$ を暗号化部324へ、ICカードの暗号鍵生成部422は $SK'$ を復号部423へ出力する。受信機の暗号化部324は通信データ $DATA$ を $SK'$ を鍵として暗号化した $Enc(SK', DATA)$ を出力し、入出力部301からICカードへ送信する。ICカードは、入出力部401が受信機から $Enc(SK', DATA)$ を受信すると、復号部423は前記保持していた $SK'$ を鍵として復号し、 $DATA$ を出力する。

【0046】このように、受信機からICカードへ発信するコマンド毎に乱数を生成し、ICカードへコマンドと共に乱数を送信し、受信機及びICカードで共通のアルゴリズムを用いて暗号鍵 $SK'$ を生成すると、コマンドの度にリフレッシュされる鍵を用いた暗号化が可能となり、セッション鍵 $SK$ を暗号鍵として用いた暗号通信と比較して、さらにセキュリティの高い暗号通信を実現できる。また、暗号鍵生成の度に $SK$ が更新されるため、たとえ乱数 $R$ が以前に用いた値と等しくなったとしても、 $SK'$ は異なり、乱数 $R$ の盗聴による $SK'$ の割り出しは困難という利点がある。

【0047】なお、必ずしも全てのコマンドに対して乱数を生成して暗号鍵SK'を毎回更新しなくてもよい。一定のコマンド生成回数もしくは一定の時間が経過したタイミングで乱数を生成するようにしてもよい。受信機からのコマンドに乱数が含まれない場合は、受信機及びICカードの復号部及び暗号化部は、既に保持しているSK'を用いて暗号通信してもよい。この場合、受信機及びICカードにおいて、暗号鍵生成処理及びSK更新処理を省略することができる。

【0048】図12は、受信装置の認証処理の後に受信機がスクランブル鍵Ksを保持するまでの処理を時系列に示すタイミングチャート図である。放送局は予め、受信機メーカー毎に、1つのICカードに対する認証情報Cijをn×m個保持している。受信機は予め、自メーカーのデバイス鍵Kdiをn個保持している。ICカードは予め、ICカード固有鍵KICjをm個と、個別鍵Kmiを保持している。

【0049】まず、受信装置認証フェーズについて説明する。受信機は、放送局から送出されたCijを受信すると、ICカードに送信する。ICカードはCijを受信すると、フィルタリング処理を行ってC'ijを生成し、受信機に送信する。受信機はC'ijを受信すると、Kdiを用いて復号し、KICjを取得する。受信機とICカードは、共有できたKICjを用いて相互認証を行い、セッション鍵SKを取得する。

【0050】次に、視聴契約更新フェーズについて説明する。視聴契約更新フェーズでは、ICカードが、EMMからスクランブル鍵Ksを復号するために必要となるワーク鍵Kwを取得する。受信機は、放送局から送出された自受信装置宛でのEMMを受信すると、ICカードに送信する。ICカードはEMMを受信すると、個別鍵Kmiを用いてEMMを復号し、ワーク鍵Kwを取得する。

【0051】次に、番組視聴フェーズについて説明する。番組視聴フェーズでは、ICカードが、ECMから番組をデスクランブルするために必要となるスクランブル鍵Ksを取得し、受信機に送信する。受信機は、放送局から送出されたECMを受信すると、ICカードに送信する。この時、乱数RもICカードに送信し、さらに、受信装置認証フェーズで得たSKとRから暗号鍵SK'を生成する。ICカードはECMを受信すると、ワーク鍵Kwを用いてECMを復号し、Ksを取得する。さらに、受信した乱数Rと、受信装置認証フェーズで得たSKとから暗号鍵SK'を生成し、Ksを暗号化して受信機に送信する。受信機は受信した暗号化済みKsを受信すると、前記生成したSK'を用いて復号し、Ksを得る。以降、受信機は、放送局から送出されるECMを受信する度に同様の処理を行い、Ksを取得する。その際、値の異なる乱数(R', R'', ...)が用いられ、また、暗号鍵SK'も毎回異なるもの(SK',

SK'', ...)に更新されていく。

【0052】なお、視聴契約更新フェーズは、一度実行されると、視聴契約を更新するまでは実行されなくてもよい。これまでに説明のあった受信装置が受信する放送波の放送形態は、地上放送、衛星放送、有線放送(CATV)のいずれであってもよい。また、その他の放送形態であってもよい。

【0053】

【発明の効果】以上の説明から明らかなように、本発明の限定受信装置認証方法及び限定受信装置では、放送波を使って受信装置認証情報を受信装置に送ることにより、ICカードが予め保持しているICカード固有鍵KICjを受信機が保持できるため、受信機とICカードとで予めグローバルシークレットを共有せずとも共有情報を安全に共有することができる。前記共有情報を用いて、認証処理を行うことにより、認証処理の都度更新されるセッション鍵SKを生成することができ、SKを用いてスクランブル鍵Ksを暗号化して、Ksを安全に受信機に送ることが可能となる。さらに、受信機からICカードへ対するコマンド毎に乱数を送信することにより、受信機及びICカードがそれぞれ前記乱数とSKとからコマンド毎に異なる暗号鍵SK'を生成して共有することができ、コマンドに対するICカードからのレスポンスデータや受信装置本体からICカードへの通信データを暗号化して、安全なデータの受け渡しが可能となる。

【0054】また、ICカード固有鍵を1つのICカードにおいて複数保持できる方式であるため、相互認証時の通信データから最初のICカード固有鍵を割り出されたとしても、別のICカード固有鍵に対応する受信装置認証情報を放送局から送出することにより、Ksを不正に取得されることを防ぐことができる。また、ICカード固有鍵は全てのICカードで異なっているため、万が一、あるICカードのICカード固有鍵の値が全て割り出されたとしても、限定受信システム運用への影響は軽微である。

【図面の簡単な説明】

【図1】従来の限定受信システムの送信側の構成を示すブロック図

【図2】従来の限定受信装置の構成を示すブロック図

【図3】本発明のデバイス鍵及びICカード固有鍵をそれぞれ受信機及びICカードに格納する手順の一例を示す図

【図4】本発明の受信装置認証情報を生成する方法を示すブロック図

【図5】本発明の限定受信装置認証方法を用いた限定受信システムにおける送信側の構成を示すブロック図

【図6】本発明の限定受信装置が認証処理を行う方法を示すブロック図

【図7】従来の相互認証方法の一例を示すブロック図

【図8】本発明の限定受信装置がICカードに受信装置認証情報記憶部を具備した場合の認証処理を行う方法を示すブロック図

【図9】本発明の限定受信装置認証方法の手順を示すフローチャート

【図10】本発明の限定受信装置が受信装置本体に受信装置認証情報フィルタリング部を具備した場合の認証方法を示すブロック図

【図11】本発明の限定受信装置がコマンド毎に乱数を生成してICカードに送信し、暗号鍵を生成して暗号通信を行う方法を示すブロック図

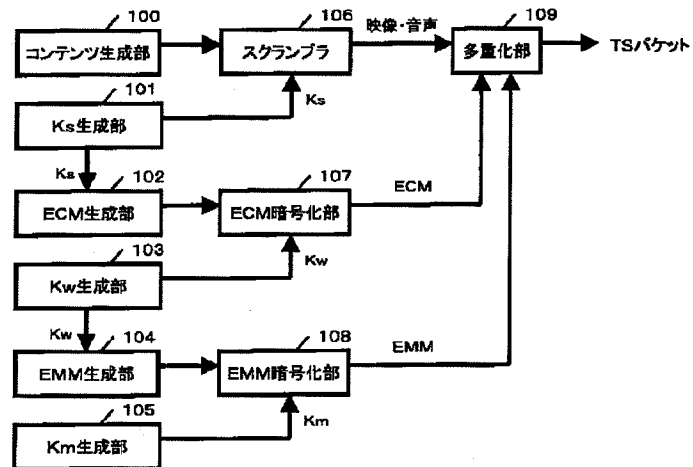
【図12】本発明の限定受信装置認証方法を用いた限定受信システムにおいて、受信装置の認証処理の後に受信機がスクランブル鍵Ksを保持するまでの処理を時系列に示すタイミングチャート

【符号の説明】

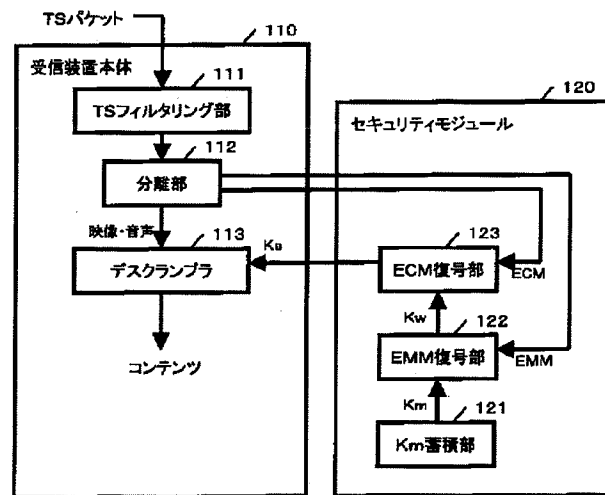
100 コンテンツ生成部  
101 Ks生成部  
102 ECM生成部  
103 Kw生成部  
104 EMM生成部  
105 Km生成部  
106 スクランプラ  
107 ECM暗号化部  
108 EMM暗号化部  
109 多重化部  
110 受信装置本体  
111 TSフィルタリング部  
112 分離部  
113 デスクランブラ  
120 セキュリティモジュール  
121 Km蓄積部  
122 EMM復号部  
123 ECM復号部  
130 (C<sub>ij</sub>, i, j) 生成部  
131 多重化部  
200 放送局  
201 鍵管理センタ  
202 デバイス鍵生成部  
203 デバイス鍵DB  
204 ICカード固有鍵生成部

205 ICカード固有鍵DB  
206 受信機メーカー  
207 受信機  
208 ICカードメーカー  
209 ICカード  
210 受信装置認証情報生成部  
211 暗号化部  
300 受信機  
301 入出力部  
302 TSフィルタリング部  
303 分離部  
304 メーカーID記憶部  
305 デバイス鍵記憶部  
306 認証情報復号部  
307 認証処理部  
308 復号部  
309 受信装置認証情報フィルタリング部  
310 相互認証部  
320 SK記憶部  
321 乱数生成部  
322 コマンド生成部  
323 暗号鍵生成部  
324 暗号化部  
400 ICカード  
401 入出力部  
402 メーカーID記憶部  
403 カードID記憶部  
404 受信装置認証情報フィルタリング部  
405 ICカード固有鍵記憶部  
406 認証処理部  
407 暗号化部  
408 Km蓄積部  
409 EMM復号部  
410 ECM復号部  
411 受信装置認証情報記憶部  
412 受信装置認証情報フィルタリング部  
413 相互認証部  
420 SK記憶部  
421 コマンド解析部  
422 暗号鍵生成部  
423 復号部

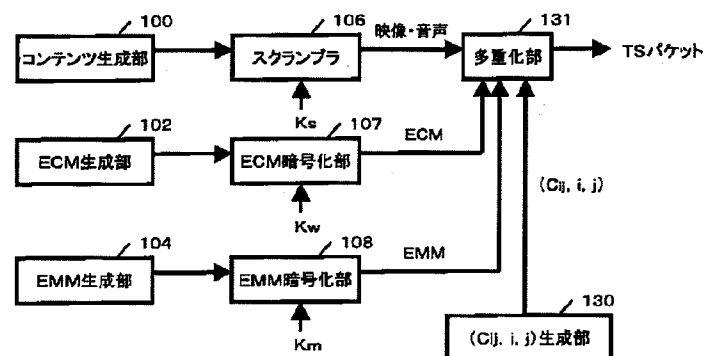
【図1】



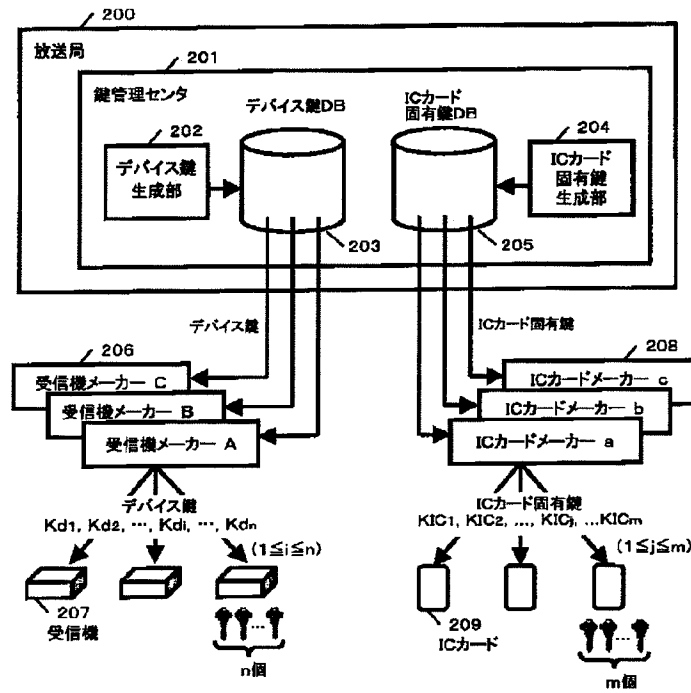
【図2】



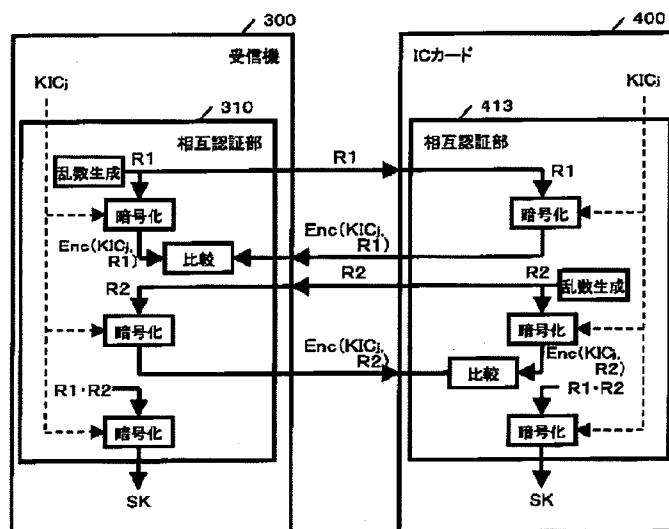
【図5】



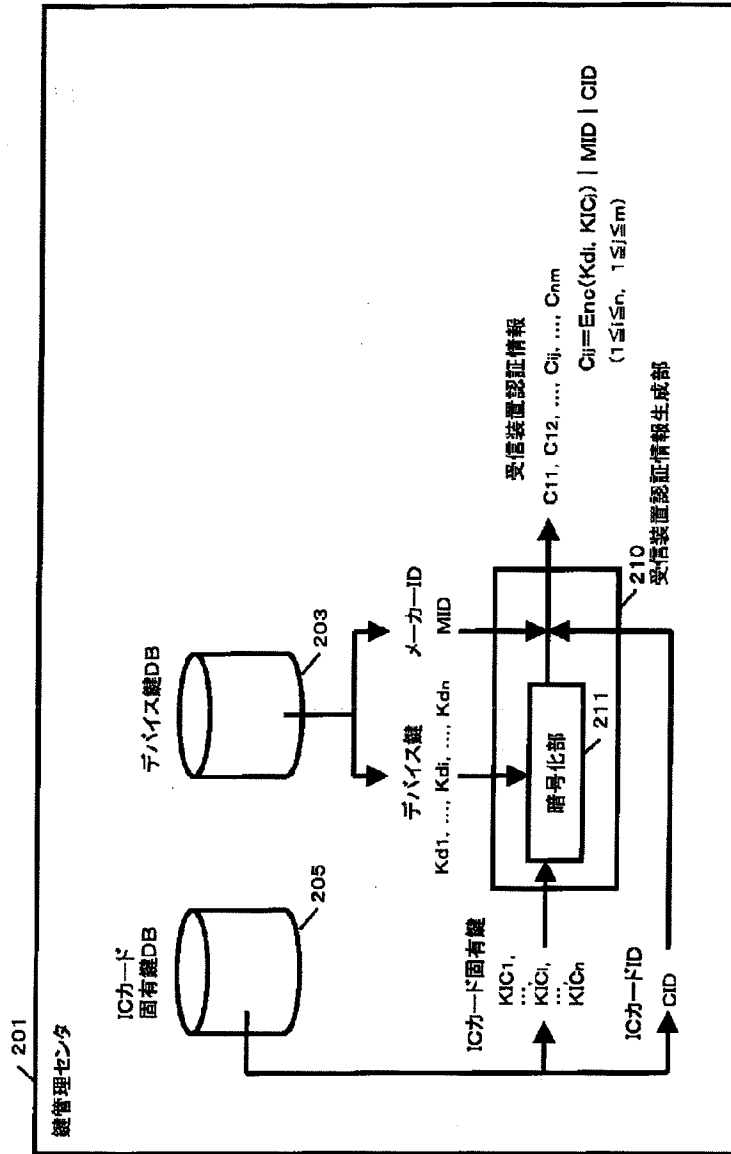
【図3】



【図7】

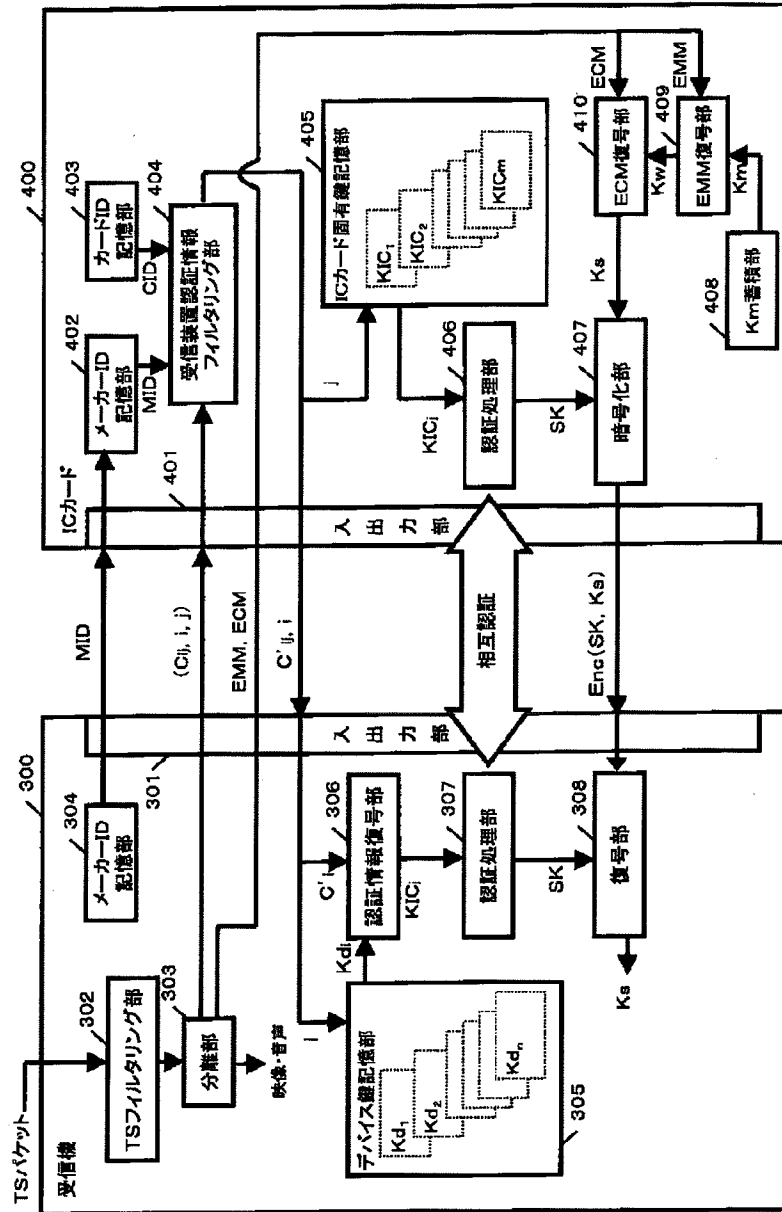


【図4】

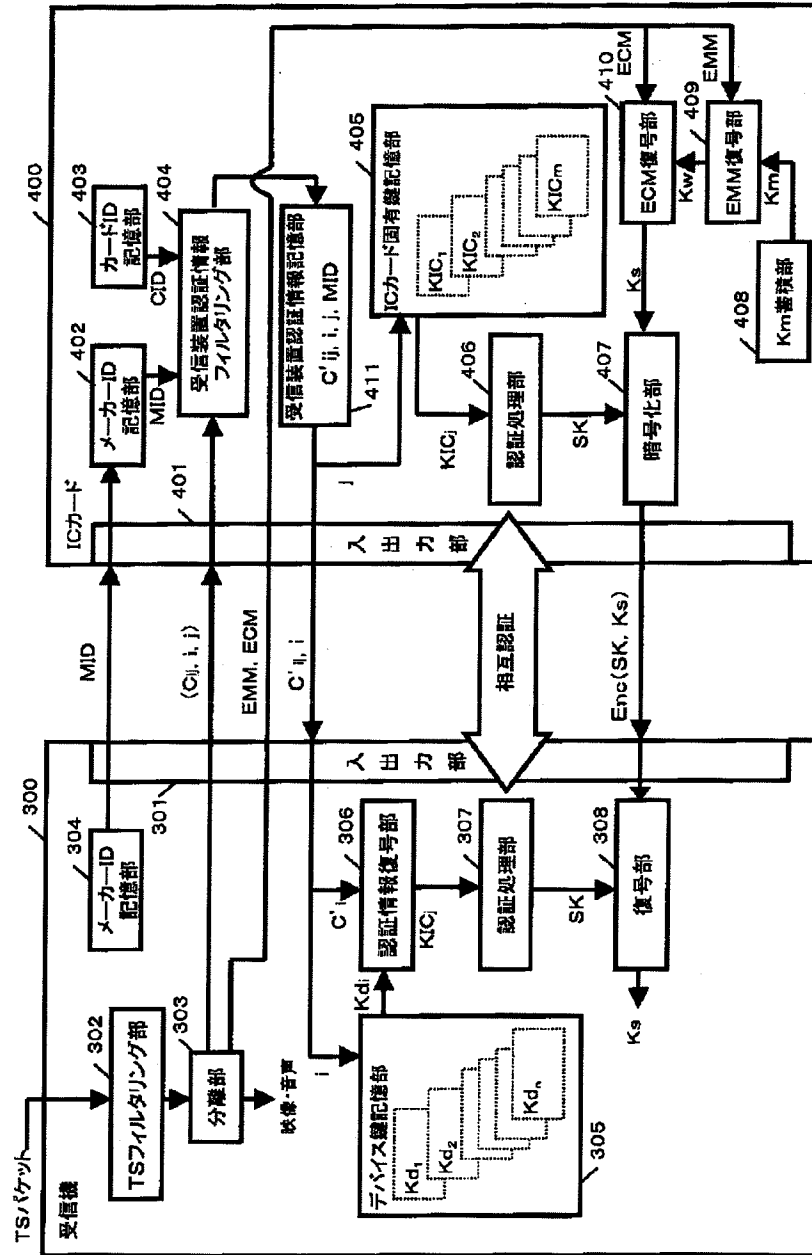




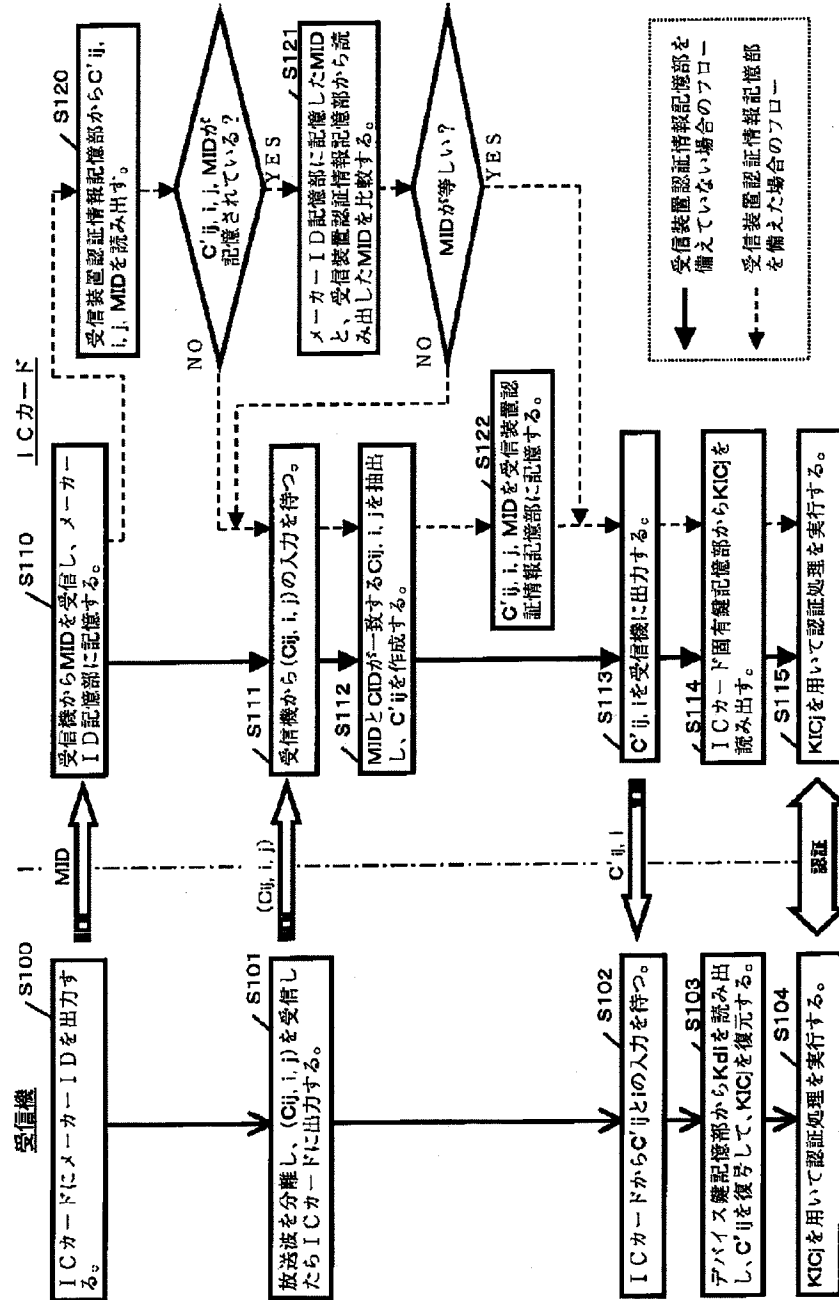
【図6】



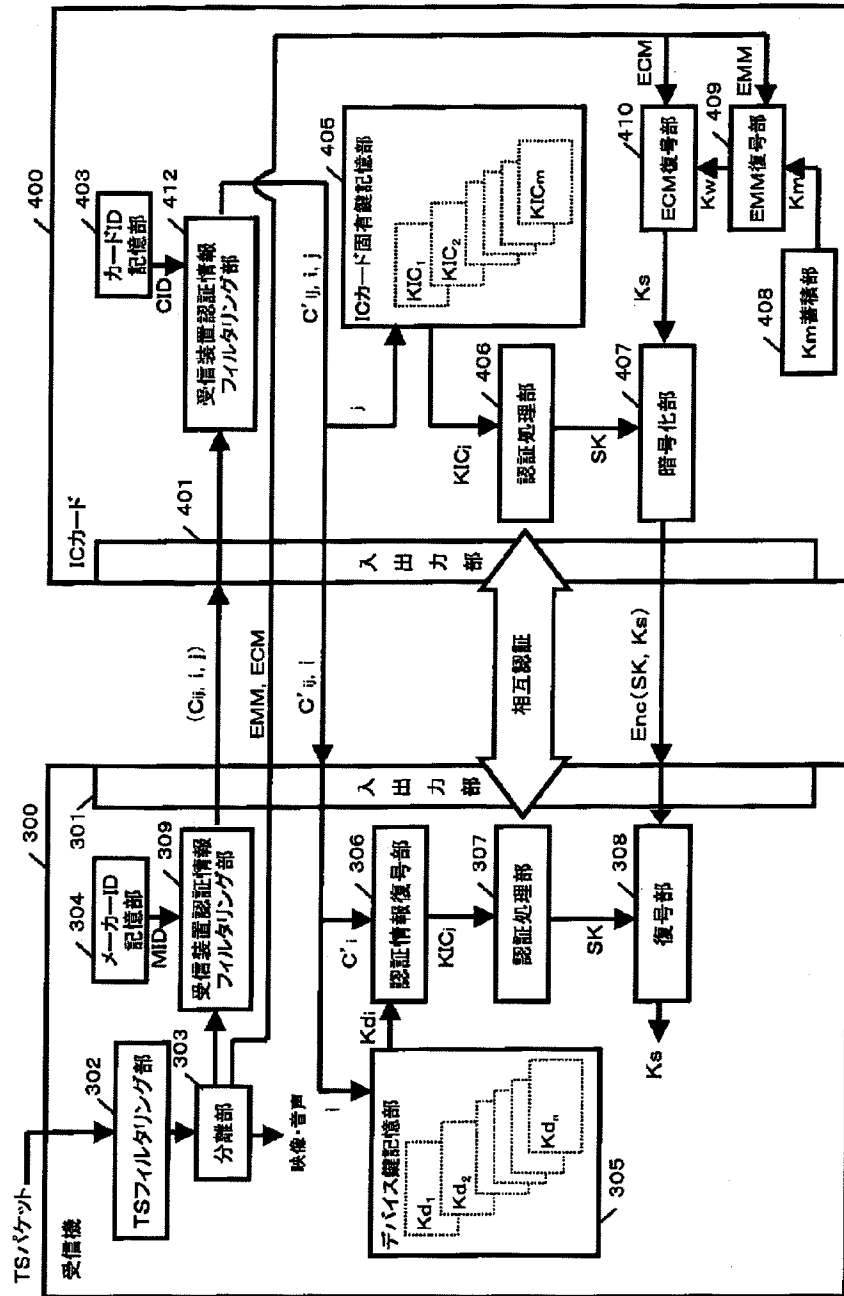
【図8】



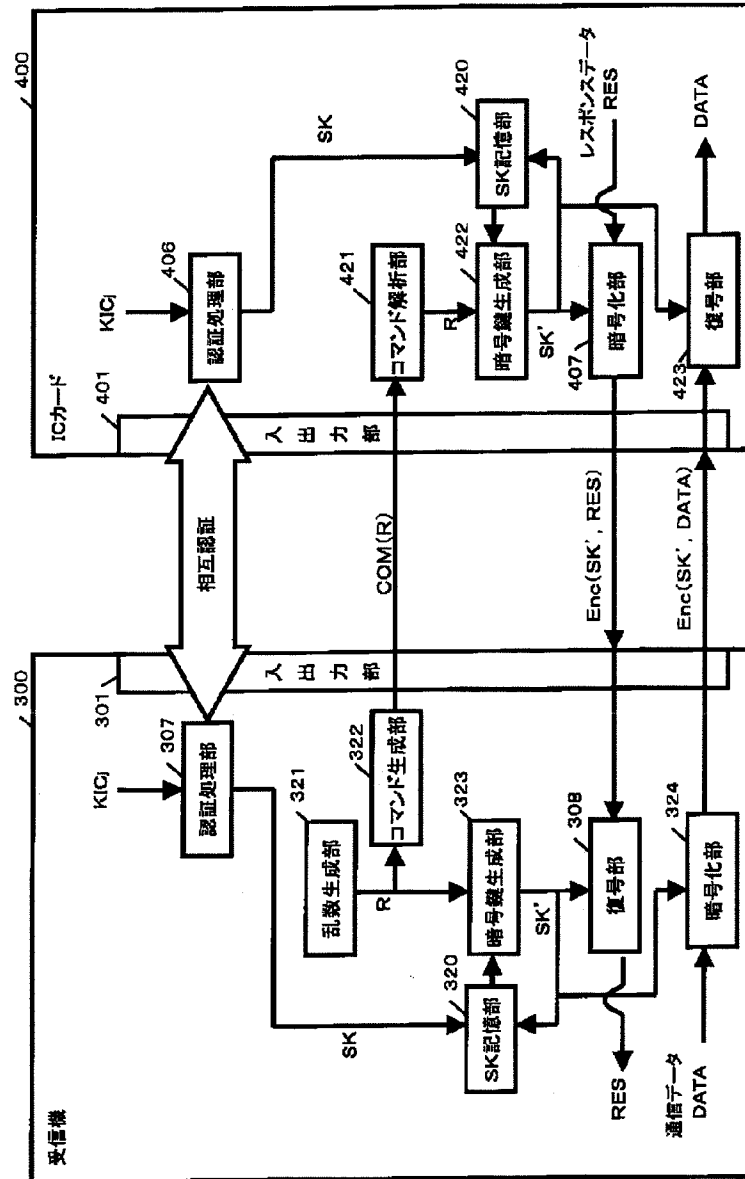
【図9】



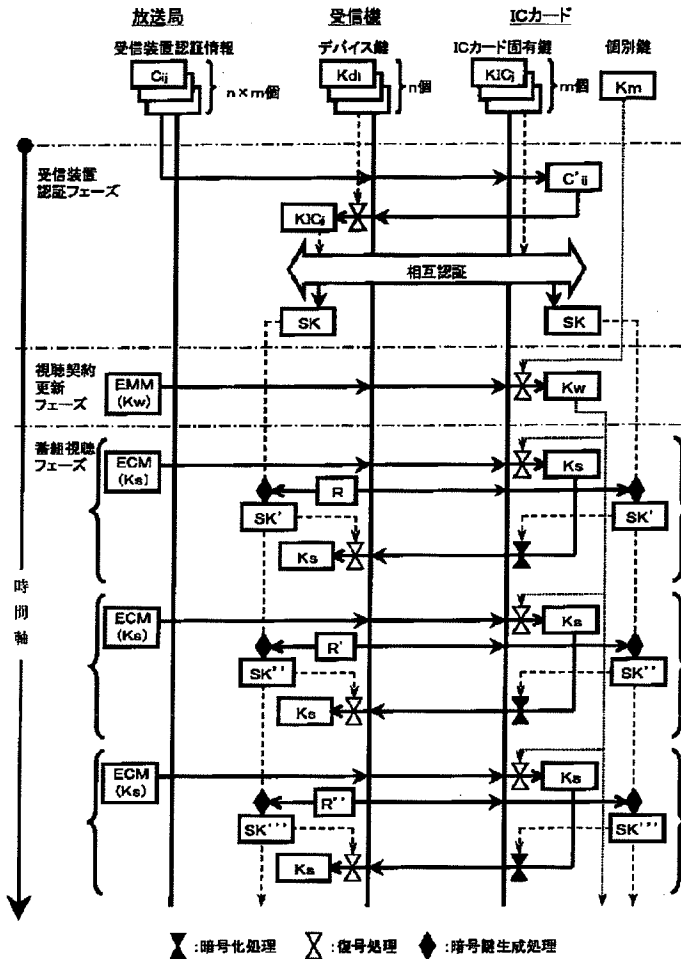
【図10】



【図11】



【図12】



フロントページの続き

(72)発明者 黒岩 渉

神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内

(72)発明者 熊崎 洋児

愛知県名古屋市中区栄2丁目6番1号 白川ビル別館5階 株式会社松下電器情報システム名古屋研究所内

(72)発明者 西條 猛

愛知県名古屋市中区栄2丁目6番1号 白川ビル別館5階 株式会社松下電器情報システム名古屋研究所内

(72)発明者 井上 哲也

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 松尾 隆史

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 村上 弘規

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 布田 裕一

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 大森 基司

大阪府門真市大字門真1006番地 松下電器産業株式会社内

F ターム(参考) 5C064 CA14 CB01 CB08 CC01 CC04  
5J104 AA07 AA16 EA04 EA22 EA24  
KA02 KA04 NA03 NA35 NA36  
NA37 NA41 NA42 PA05

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成19年11月29日(2007.11.29)

【公開番号】特開2002-152194(P2002-152194A)

【公開日】平成14年5月24日(2002.5.24)

【出願番号】特願2000-344384(P2000-344384)

【国際特許分類】.

H O 4 L 9/32 (2006.01)

H O 4 H 1/00 (2006.01)

H O 4 H 1/02 (2006.01)

H O 4 L 9/08 (2006.01)

H O 4 N 7/167 (2006.01)

【F I】

H O 4 L 9/00 6 7 5 A

H O 4 H 1/00 F

H O 4 H 1/02 E

H O 4 L 9/00 6 0 1 C

H O 4 N 7/167 Z

【手続補正書】

【提出日】平成19年10月15日(2007.10.15)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムの限定受信装置であって、

前記セキュリティモジュールとのデータ入出力を行う入出力手段と、

1つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、

前記1つ以上の限定受信装置固有情報のうちの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記入出力手段を介して入力される暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段と

を具備することを特徴とする限定受信装置。

【請求項2】

限定受信装置のメーカーを識別するメーカーIDを記憶するメーカーID記憶手段と、

前記メーカーIDを参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段と

を具備することを特徴とする請求項1に記載の限定受信装置。

【請求項3】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムのセキュリティモジ



ジュールであって、

前記限定受信装置とのデータ入出力を行う入出力手段と、

セキュリティモジュールを一意に識別するセキュリティモジュール I D を記憶するセキュリティモジュール I D 記憶手段と、

前記セキュリティモジュール I D を参照して、前記限定受信装置から前記入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1 つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記 1 つ以上のセキュリティモジュール固有情報のうちのセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と

を具備することを特徴とするセキュリティモジュール。

【請求項 4】

前記セキュリティモジュールは I C カードであり、前記セキュリティモジュール I D はカード I D である、請求項 3 記載のセキュリティモジュール。

【請求項 5】

前記限定受信装置から前記入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカー I D を記憶するメーカー I D 記憶手段をさらに具備し、

前記フィルタリング手段は、前記メーカー I D と前記カード I D とを参照して、前記限定受信装置から前記入出力手段を介して入力される受信装置認証情報をフィルタリングすることを特徴とする請求項 4 に記載のセキュリティモジュール。

【請求項 6】

前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項 3 から請求項 5 のいずれか一項に記載のセキュリティモジュール。

【請求項 7】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、

前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、

限定受信装置のメーカーを識別するメーカー I D を記憶するメーカー I D 記憶手段と、

1 つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、

前記 1 つ以上の限定受信装置固有情報のうちの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、

前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、

セキュリティモジュールを一意に識別するセキュリティモジュール I D を記憶するセキュリティモジュール I D 記憶手段と、

前記限定受信装置から前記第二入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカー I D を記憶するメーカー I D 記憶手段と、

前記メーカー I D と前記セキュリティモジュール I D とを参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1 つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記 1 つ以上のセキュリティモジュール固有情報のうちのセキュリティモジュール固

有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と

を具備することを特徴とする限定受信システム。

【請求項 8】

前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項 7 に記載の限定受信システム。

【請求項 9】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、

前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、

限定受信装置のメーカーを識別するメーカー ID を記憶するメーカー ID 記憶手段と、前記メーカー ID を参照して、受信した放送波に含まれる受信装置認証情報をフィルタリングするフィルタリング手段と、

1 つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、

前記 1 つ以上の限定受信装置固有情報のうちの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段とを具備し、

前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、

セキュリティモジュールを一意に識別するセキュリティモジュール ID を記憶するセキュリティモジュール ID 記憶手段と、

前記セキュリティモジュール ID を参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1 つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記 1 つ以上のセキュリティモジュール固有情報のうちのセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値を出力する認証処理手段と

を具備することを特徴とする限定受信システム。

【請求項 10】

前記セキュリティモジュールは、前記フィルタリング手段が出力した受信装置認証情報を記憶する受信装置認証情報記憶手段をさらに具備することを特徴とする請求項 9 に記載の限定受信システム。

【請求項 11】

セキュリティモジュールが装着されている限定受信装置の認証方法であって、  
前記限定受信装置が、  
受信した放送波に含まれる受信装置認証情報を分離するステップと、  
自受信装置宛の受信装置認証情報だけを取り出すフィルタリング処理ステップと、  
前記受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成するステップと、  
前記限定受信装置と前記セキュリティモジュールとが、  
前記限定受信装置と前記セキュリティモジュールとが共有した前記セキュリティモジュール固有情報を用いて認証処理を行うステップを有することを特徴とする限定受信装置認証方法。

【請求項 12】

前記受信装置認証情報は、前記限定受信装置が1つ以上保持する限定受信装置固有情報のいずれか1つを鍵として、前記セキュリティモジュールが1つ以上保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報のいずれか1つを暗号化することにより生成される情報と、限定受信装置のメーカーを識別するメーカーIDと、セキュリティモジュールを識別するセキュリティモジュールIDとを含み、

受信装置認証情報の生成に用いた限定受信装置固有情報及びセキュリティモジュール固有情報を特定するためのインデックス情報に組み合わせて、放送局設備から放送波を用いて送出されることを特徴とする、請求項11に記載の限定受信装置認証方法。

【請求項13】

前記フィルタリング処理は、前記メーカーIDと前記セキュリティモジュールが記憶しているセキュリティモジュールIDとが一致する受信装置認証情報を自受信装置宛の受信装置認証情報として選択することを特徴とする請求項11及び請求項12のいずれか一項に記載の限定受信装置認証方法。

【請求項14】

前記限定受信装置で生成される前記共有情報は、前記限定受信装置固有情報を鍵として、前記受信装置認証情報に含まれる情報を復号することにより復元されることを特徴とする、請求項11から請求項13のいずれか一項に記載の限定受信装置認証方法。

【請求項15】

前記フィルタリング処理は、前記限定受信装置において、当該限定受信装置が記憶しているメーカーIDと一致する受信装置認証情報を選択し、前記セキュリティモジュールにおいて、当該セキュリティモジュールが記憶しているセキュリティモジュールIDと一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項11から請求項14のいずれか一項に記載の限定受信装置認証方法。

【請求項16】

前記セキュリティモジュールは、当該セキュリティモジュールが前記限定受信装置に装着された後に前記限定受信装置から入力されるメーカーIDを記憶するステップを有することを特徴とする、請求項11から請求項14のいずれか一項に記載の限定受信装置認証方法。

【請求項17】

前記フィルタリング処理は、前記セキュリティモジュールにおいて、前記記憶されたメーカーIDと前記セキュリティモジュールが記憶しているセキュリティモジュールIDとが一致する受信装置認証情報を選択することにより自受信装置宛の受信装置認証情報を抽出することを特徴とする、請求項16に記載の限定受信装置認証方法。

【請求項18】

前記セキュリティモジュールは、フィルタリング処理により抽出した受信装置認証情報を記憶するステップを有し、

前記セキュリティモジュールが前記限定受信装置に装着された後に前記限定受信装置から入力されるメーカーIDが前記記憶している受信装置認証情報に含まれるメーカーIDと等しい場合は、前記記憶している受信装置認証情報を前記限定受信装置に出力し、

前記限定受信装置は、前記セキュリティモジュールから渡された前記受信装置認証情報を基に前記共有情報を生成することを特徴とする、請求項15から請求項17のいずれか一項に記載の限定受信装置認証方法。

【請求項19】

前記認証処理手段が出力した前記セキュリティモジュールとの共有値を記憶する記憶手段と、

乱数を出力する乱数生成手段と、

前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて前記セキュリティモジュールから前記入出力手段を介して入力され

る情報を復号する復号手段と

をさらに具備することを特徴とする、請求項 1 及び請求項 2 のいずれか一項に記載の限定受信装置。

【請求項 20】

前記暗号鍵を用いて前記セキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備することを特徴とする、請求項 19 に記載の限定受信装置。

【請求項 21】

前記認証処理手段が出力した前記限定受信装置との共有値を記憶する記憶手段と、  
前記記憶している共有値と前記限定受信装置から前記入出力手段を介して入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて前記限定受信装置へ出力する情報を暗号化する暗号化手段と  
をさらに具備することを特徴とする、請求項 3 から請求項 6 のいずれか一項に記載のセキュリティモジュール。

【請求項 22】

前記暗号鍵を用いて前記限定受信装置から前記入出力手段を介して入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項 21 に記載のセキュリティモジュール。

【請求項 23】

放送されてきた信号を受信してセキュリティモジュールに出力する限定受信装置と、前記限定受信装置から入力されたデータを処理して当該限定受信装置に処理データを出力する前記セキュリティモジュールとを構成要素に含む限定受信システムであって、

前記限定受信装置は、前記セキュリティモジュールとのデータ入出力を行う第一入出力手段と、

限定受信装置のメーカーを識別するメーカー ID を記憶するメーカー ID 記憶手段と、  
1 つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、

前記 1 つ以上の限定受信装置固有情報のうちの限定受信装置固有情報を鍵として、前記セキュリティモジュールから前記第一入出力手段を介して入力される暗号化されている情報を復号する復号手段と、

前記復号手段が出力する情報を入力として前記セキュリティモジュールとの認証処理を行い、前記セキュリティモジュールとの共有値を出力する認証処理手段と、

前記認証処理手段が出力したセキュリティモジュールとの共有値を記憶する記憶手段と

、  
乱数を出力する乱数生成手段と、

前記記憶している共有値と前記乱数とを入力として暗号鍵を出力する暗号鍵生成手段と

、  
前記暗号鍵を用いて前記セキュリティモジュールから前記第一入出力手段を介して入力される情報を復号する復号手段とを具備し、

前記セキュリティモジュールは、前記限定受信装置とのデータ入出力を行う第二入出力手段と、

セキュリティモジュールを一意に識別するセキュリティモジュール IDを記憶するセキュリティモジュール ID 記憶手段と、

前記限定受信装置から前記第二入出力手段を介して入力される、前記限定受信装置のメーカーを識別するメーカー ID を記憶するメーカー ID 記憶手段と、

前記メーカー ID と前記セキュリティモジュール ID とを参照して、前記限定受信装置から前記第二入出力手段を介して入力される受信装置認証情報をフィルタリングするフィルタリング手段と、

1 つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、

前記 1 つ以上のセキュリティモジュール固有情報のうちのセキュリティモジュール固有情報を入力として前記限定受信装置との認証処理を行って前記限定受信装置との共有値

を出力する認証処理手段と、

前記認証処理手段が出力した限定受信装置との共有値を記憶する記憶手段と、

前記記憶している共有値と前記限定受信装置から前記第二入出力手段を介して入力される乱数とを入力として暗号鍵を出力する暗号鍵生成手段と、

前記暗号鍵を用いて前記限定受信装置へ出力する情報を暗号化する暗号化手段とを具備することを特徴とする限定受信システム。

【請求項 24】

前記限定受信装置は、前記暗号鍵を用いて前記セキュリティモジュールへ出力する情報を暗号化する暗号化手段をさらに具備し、

前記セキュリティモジュールは、前記暗号鍵を用いて前記限定受信装置から前記第二入出力手段を介して入力される情報を復号する復号手段をさらに具備することを特徴とする、請求項 23 に記載の限定受信システム。

【請求項 25】

セキュリティモジュールが装着されている限定受信装置と前記セキュリティモジュール間の暗号通信方法であって、

前記限定受信装置は、前記セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップを有し、

前記セキュリティモジュールは、前記限定受信装置との認証処理によって生成した共有値を記憶するステップを有し、

前記限定受信装置及び前記セキュリティモジュールは、それぞれが記憶した共有値を鍵として用いて暗号通信を行うことを特徴とする、暗号通信方法。

【請求項 26】

セキュリティモジュールが装着されている限定受信装置と前記セキュリティモジュール間の暗号通信方法であって、

前記限定受信装置は、前記セキュリティモジュールとの認証処理によって生成した共有値を記憶するステップと、

乱数を生成するステップと、

前記乱数を前記セキュリティモジュールに出力するステップと、

前記記憶したセキュリティモジュールとの共有値と前記乱数とを用いて暗号鍵を生成するステップとを有し、

前記セキュリティモジュールは、前記限定受信装置との認証処理によって生成した共有値を記憶するステップと、

前記記憶した限定受信装置との共有値と前記限定受信装置から入力された乱数とを用いて暗号鍵を生成するステップと、

前記暗号鍵を前記限定受信装置との共有値として記憶するステップとを有し、

前記限定受信装置及び前記セキュリティモジュールは、それぞれが生成した暗号鍵を用いて暗号通信を行うことを特徴とする、暗号通信方法。

【請求項 27】

前記限定受信装置は、前記生成した暗号鍵を前記セキュリティモジュールとの新しい共有値として記憶するステップをさらに有し、

前記セキュリティモジュールは、前記生成した暗号鍵を前記限定受信装置との新しい共有値として記憶するステップをさらに有することを特徴とする、請求項 26 に記載の暗号通信方法。

【請求項 28】

前記限定受信装置から前記セキュリティモジュールへのコマンド送信をトリガーとして、前記限定受信装置が前記乱数を生成することを特徴とする、請求項 26 及び請求項 27 のいずれか一項に記載の暗号通信方法。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】限定受信システムの限定受信装置及びセキュリティモジュール、限定受信システム、限定受信装置認証方法及び暗号通信方法

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正の内容】

【0001】

【発明の属する技術分野】

本発明は、視聴契約を必要とする放送システム（限定受信システム）に関し、特に、限定受信システムを構成する限定受信装置とセキュリティモジュールとの間で安全に暗号通信を行う技術に関する。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正の内容】

【0005】

多重化部で多重化された信号はTSパケット（Transport Stream Packet）に変換されて送出される。一方、番組を視聴する受信側の構成は、図2に示すように、限定受信装置（受信機）110と、受信機に装着されるICカード等のセキュリティモジュール120とを備えており、受信機は選局されたTSパケットだけを取り込むTSフィルタリング部111と、多重されている信号を分離する分離部112と、スクランブルされたコンテンツを復号化するデスクランブラ113とを具備し、また、セキュリティモジュールは、Kmを保持するKm蓄積部121と、Kmを用いてEMMを復号するEMM復号部122と、Kwを用いてECMを復号するECM復号部123とを具備している。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

【発明が解決しようとする課題】

これまでの説明から明らかなように、限定受信装置とセキュリティモジュールとの間で安全な暗号通信を行うためには、限定受信装置とセキュリティモジュールとが、共有情報を安全に共有することが重要である。予め共有情報をグローバルシークレットとして限定受信装置とセキュリティモジュールとに格納した場合、セッション毎に相互認証を行うことにより、セッション毎に異なる安全なセッション鍵を共有することが可能である。しかし、この場合、悪意を持つ者が限定受信装置とセキュリティモジュールとの間で通信される相互認証用データ（チャレンジ・レスポンス等）を不正取得して暗号解読を試み、万が一、共有情報の割り出しに成功すると、セッション鍵の割り出しが可能となり、その結果、スクランブル鍵Ksや、視聴契約情報、課金情報といった限定受信装置とセキュリティモジュールとの間で通信されるデータが不正に取得されてしまう。また、割り出された共有情報は、全ての受信装置において共通であるため、限定受信システム運用に与えるダメージは非常に重大である。システム運用を回復するための対処として、新しい共有情報を暗号化して格納した記憶メディアを全視聴者に配布して受信機及びセキュリティモジュールの共有情報を更新する方法が考えられるが、これは膨大なコストの発生を伴うと予想され、非現実的である。

## 【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

また、限定受信装置とICカード等のセキュリティモジュールの製造は、それぞれ複数の異なるメーカーが担当するのが一般的である。予め共有情報を限定受信装置及びセキュリティモジュールに格納しておく場合、全てのメーカー製の限定受信装置と、全てのメーカー製のセキュリティモジュールとの組み合わせにおいて相互認証を正しく行うためには、メーカーを問わず、全ての限定受信装置及びセキュリティモジュールで等しい共有情報を共有する必要がある。この場合、ある1つのメーカーにおける機密情報管理レベルが低く、メーカー内部から共有情報の漏洩が発生してしまうと、他のメーカー製の限定受信装置及びセキュリティモジュールにもその影響が波及し、限定受信システムの運用に致命的なダメージを及ぼすことになる。

## 【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

本発明は、こうした問題点を解決するものであり、限定受信装置とセキュリティモジュールとで予め共通の共有情報を持たずとも、セッション鍵生成等で用いる共有情報を安全に共有することができる限定受信システムの限定受信装置及びセキュリティモジュール、限定受信システム、限定受信装置の認証方法、及び、暗号通信方法を提供することを目的とする。

## 【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

## 【課題を解決するための手段】

この課題を解決するために本発明は、限定受信装置にセキュリティモジュールが装着される構成を取る限定受信システムにおいて、限定受信装置は限定受信装置を製造するメーカーを識別するIDを記憶するメーカーID記憶手段と、1つ以上の限定受信装置固有情報を記憶する限定受信装置固有情報記憶手段と、前記1つ以上の限定受信装置固有情報のうちの限定受信装置固有情報を鍵として暗号化されている情報を復号する復号手段と、前記復号手段が出力する情報を入力としてセキュリティモジュールとの認証処理を行う認証処理手段とを備え、セキュリティモジュールはセキュリティモジュールを一意に識別するセキュリティモジュールIDを記憶するセキュリティモジュールID記憶手段と、前記メーカーIDと前記セキュリティモジュールIDとを参照して受信装置認証情報をフィルタリングするフィルタリング手段と、1つ以上のセキュリティモジュール固有情報を記憶するセキュリティモジュール固有情報記憶手段と、前記1つ以上のセキュリティモジュール固有情報のうちのセキュリティモジュール固有情報を入力として限定受信装置との認証処理を行う認証処理手段を備えることを特徴とする。

## 【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

## 【補正の内容】

## 【0014】

また、放送局設備において受信装置認証情報を生成し、受信装置認証情報を放送局から放送波を用いて送出し、限定受信装置は受信した受信装置認証情報からメーカーIDとセキュリティモジュールIDを検索キーとして自受信装置宛の受信装置認証情報だけをフィルタリングし、フィルタリングした受信装置認証情報を基にセキュリティモジュールが予め保持しているセキュリティモジュール固有情報に等しい共有情報を生成して、限定受信装置とセキュリティモジュールは前記共有情報を用いて認証処理を行う。

## 【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

## 【補正の内容】

## 【0015】

また、受信装置認証情報は、限定受信装置が保持する限定受信装置固有情報を鍵としてセキュリティモジュールが保持するセキュリティモジュール毎に固有のセキュリティモジュール固有情報を暗号化することにより生成される情報と、限定受信装置のメーカーを識別するメーカーIDと、セキュリティモジュールを識別するセキュリティモジュールIDとから構成される。

## 【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

## 【補正の内容】

## 【0016】

以上により、限定受信装置とセキュリティモジュールとでセキュリティモジュール固有情報を共有し、その共有情報を基に、限定受信装置とセキュリティモジュールとの間の暗号通信に用いるセッション鍵を生成する。また、限定受信装置は乱数生成手段と、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備え、セキュリティモジュールは、セッション鍵記憶手段と、暗号鍵生成手段と、暗号化手段と、復号手段を備える。

## 【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

## 【補正の内容】

## 【0017】

また、限定受信装置は乱数を生成してセキュリティモジュールに出力すると共に、セッション鍵記憶手段から読み出したセッション鍵と前記乱数とから暗号鍵を生成する。さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。セキュリティモジュールは、限定受信装置から入力した乱数と、セッション鍵記憶手段から読み出したセッション鍵とから暗号鍵を生成する、さらに、生成した暗号鍵を新しいセッション鍵としてセッション鍵記憶手段に記憶する。

## 【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

## 【補正の内容】

## 【0018】

以上により、限定受信装置とセキュリティモジュールとで共通の暗号鍵を共有し、暗号



通信を行う。

【手続補正 1 4】

【補正対象書類名】明細書

【補正対象項目名】0 0 1 9

【補正方法】変更

【補正の内容】

【0 0 1 9】

【発明の実施の形態】

本発明の実施の形態について、図を用いて説明する。なお、以降では、限定受信装置を受信機、セキュリティモジュールをＩＣカード、限定受信装置固有情報をデバイス鍵、セキュリティモジュール固有情報をＩＣカード固有鍵と記述して説明する。